CLAIMS

What is claimed is:

1. A method of secure communication, comprising:

receiving a request for a data transaction from a client lacking hardware cryptography functionality, together with security parameters specific to the client, at a server through a secure connection between the client and the server;

performing any necessary security processing for the requested data transaction within the server on behalf of the client utilizing hardware cryptography functionality available within the server; and

after performing any necessary security processing on the requested data transaction, forwarding the processed data transaction to a target of the requested data transaction as if originating from the client.

2. The method of claim 1, wherein the step of receiving a request for a data transaction from a client lacking hardware cryptography functionality, together with security parameters specific to the client, at a server through a secure connection between the client and the server further comprises:

receiving the requested data transaction through an IPSEC connection.

3. The method of claim 1, wherein the step of receiving a request for a data transaction from a client lacking hardware cryptography functionality, together with security parameters specific to the client, at a server through a secure connection between the client and the server further comprises:

receiving encryption keys or a digital certificate assigned to the client.

4. The method of claim 1, wherein the step of performing any necessary security processing for the requested data transaction within the server on behalf of the client utilizing hardware cryptography functionality available within the server further comprises:

encrypting data within the requested data transaction; or

generating a digital signature for attachment to the data transaction.

5. The method of claim 1, wherein the step of forwarding the processed data transaction to a target of the requested data transaction as if originating from the client further comprises:

forwarding the processed data transaction via an SSL transaction.

6. The method of claim 1, further comprising:

receiving a response to the processed data transaction at the server;

performing any security processing required by the response; and

forwarding the processed response, together with any results of the security processing, to the client via the secure connection.

7. The method of claim 6, wherein the step of performing any security processing required by the response further comprises:

decrypting the received response; or

validating a digital signature attached to the received response.

8. A system for secure communication, comprising:

a client lacking hardware cryptography functionality;

a server including hardware cryptography functionality;

a secure Internet Protocol connection between the client and the server;

means for receiving a request for a data transaction from the client, together with security parameters specific to the client, at the server through the secure connection;

means for performing any necessary security processing for the requested data transaction within the server on behalf of the client utilizing the hardware cryptography functionality available within the server; and

means, responsive to completion of performing any necessary security processing on the requested data transaction, for forwarding the processed data transaction to a target of the requested data transaction as if originating from the client.

9. The system of claim 8, wherein secure connection further comprises:

an IPSEC connection.

10. The system of claim 8, wherein the means for receiving a request for a data transaction from the client, together with security parameters specific to the client, at the server through the secure connection further comprises:

means for securely receiving encryption keys or a digital certificate assigned to the client.

11. The system of claim 8, wherein the means for performing any necessary security processing for the requested data transaction within the server on behalf of the client utilizing hardware cryptography functionality available within the server further comprises:

means for encrypting data within the requested data transaction; or

means for generating a digital signature for attachment to the data transaction.

12. The system of claim 8, wherein the means for forwarding the processed data transaction to a target of the requested data transaction as if originating from the client further comprises:

means for forwarding the processed data transaction via an SSL transaction.

13. The system of claim 8, further comprising:

means for receiving a response to the processed data transaction at the server;

means for performing any security processing required by the response; and

means for forwarding the processed response, together with any results of the security processing, to the client via the secure connection.

14. The system of claim 13, wherein the means for performing any security processing required by the response further comprises:

means for decrypting the received response; or

means for validating a digital signature attached to the received response.

15. A computer program product within a computer usable medium for secure communication, comprising:

instructions for receiving a request for a data transaction from a client lacking hardware cryptography functionality, together with security parameters specific to the client, at a server through a secure connection between the client and the server;

instructions for performing any necessary security processing for the requested data transaction within the server on behalf of the client utilizing hardware cryptography functionality available within the server; and

instructions, responsive to completion of performing any necessary security processing on the requested data transaction, for forwarding the processed data transaction to a target of the requested data transaction as if originating from the client.

16. The computer program product of claim 15, wherein the instructions for receiving a request for a data transaction from a client lacking hardware cryptography functionality, together with security parameters specific to the client, at a server through a secure connection between the client and the server further comprise:

instructions for receiving the requested data transaction through an IPSEC connection.

17. The computer program product of claim 15, wherein the instructions for receiving a request for a data transaction from a client lacking hardware cryptography functionality, together with security parameters specific to the client, at a server through a secure connection between the client and the server further comprise:

instructions for securely receiving encryption keys or a digital certificate assigned to the client.

18. The computer program product of claim 15, wherein the instructions for performing any necessary security processing for the requested data transaction within the server on behalf of the client utilizing hardware cryptography functionality available within the server further comprise:

instructions for encrypting data within the requested data transaction; or

instructions for generating a digital signature for attachment to the data transaction.

19. The computer program product of claim 15, wherein the instructions for forwarding the processed data transaction to a target of the requested data transaction as if originating from the client further comprises:

instructions for forwarding the processed data transaction via an SSL transaction.

20. The computer program product of claim 15, further comprising:

instructions for receiving a response to the processed data transaction at the server;

instructions for performing any security processing required by the response; and

instructions for forwarding the processed response, together with any results of the security processing, to the client via the secure connection.

21. The computer program product of claim 20, wherein the instructions for performing any security processing required by the response further comprise:

instructions for decrypting the received response; or

instructions for validating a digital signature attached to the received response.